#7

Certificate of Facsimile Transmission

I hereby certify that this paper is being facsimile transmitted to (703) 872-9306 at the U S. Patent and Trademark Office on January 6, 2004.

Harris A. Wolin

Attorney Docket No.: **2709/1BG (043520-00001)**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	:	Samir H. Nanavati et al.
Serial No.	:	09/311,928
Filed	:	May 14, 1999
Title	:	**Identity Verification Method ...**
Examiner	:	Norman M. Wright
Group Art Unit	:	2134
Confirmation No.	:	1907

January 6, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION UNDER 37 C.F.R. §1.131

We, Samir H. Nanavati and Raikumar H. Nanavati, inventors and applicants of the above-referenced invention and patent application, declare as follows:

1. On May 14, 1999, we filed a non-provisional patent application covering the above-referenced invention and claiming the benefit of provisional patent application 60/085,514 filed May 14, 1998.
2. Prior to April 24, 1998, we conceived of the present invention as evidenced by the attached four (4) pages of the text of an email (header removed) and diligently reduced such invention to practice through the filing of the said provisional patent application.

3. Such email pages exhibit conception of the instant invention prior to April 24, 1998 and were prepared by Samir as a result of discussions between ourselves concerning the instant invention.
4. The present invention is embodied in such attached pages as demonstrated by detailed descriptions of four scenarios in which a Central Biometric Authority (CBA) may be manifested. For example, Scenario 1 in the notes states how, as described in Claim 1, a sender sends a message to a receiver and how one of the parties, in this case the receiver, forwards a second message to the CBA. The CBA compares biometric templates and returns verification information. A receiver of a message forwards it to the CBA for biometric template comparison. Scenario 2 in the notes states how a message is synchronously encrypted as described in Claim 10. Scenario 3 states how a parent can designate his neighbor as a proxy with authority to pick up the parent's child as described in Claim 13. Scenario 4 states how CBA can be used as a third party process for verifying any claimed identity as described in Claim 12.
5. We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the Untied States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Samir H. Nanavati 1/6/04
(date)

Raikumar H. Nanavati 1/06/04
(date)

Attachment: Four (4) pages of the text of an email composed by Samir evidencing conception of the instant invention prior to April 28, 1998.

Following is an overview of some of the basic concepts related to Biometric Key Infrastructure (BKI).

The CBA:
The Central Biometric Authority must be a trusted third party. Synergy is likely if the CBA also serves as the certificate and revocation authority.

To accept a new user, the CBA must identify the user, assumedly using an identification process similar to that used when issuing the private key for the PKI.

The records on file A given user might have multiple temples on file: for different vendors/standards of the sample technology, for different sample types of the same technology (e.g., different fingers, or a different pass phrase), and different technologies]

Concepts:
Scenario 1: Sender Identification Only:-- when a customer sends a message, a biometric submission is included with the message. [note: either the full submission or measurement, e.g., minutia points of a fingerprint, of the submission are sent]. When the receiver gets the message, they forward the submission and the senders claimed name to the Central Biometric Authority. The submission is compared to the template on file and the comparison score is returned to the recipient. Depending on the verification score required by the recipient (e.g., for higher risk transactions a higher score may be required), the claimed identification of the sender can be confirmed or denied. Note that with this scenario standard PKI is utilized.

Scenario 2: Sender and Recipient Identification w/ synchronous encryption.

A message is written and encrypted with a single use synchronous key. The encrypted message and a message identifier is sent to the recipient. A message posting is sent (with PKI) to the CBA. This message posing consists of the following:
-message identifier
-biometric sample from the sender
-intended recipient's name
-synchronous key used to encrypt message

When the recipient gets the message, they submit their sample, along with the message indicator to the CBA. The CBA compares the recipient's sample to the sample on record for the intended recipient as stated in the message posting. The CBA also compares the sender's submitted sample to that on record. If both samples match, the receiver is sent (with PKI) the synchronous key, and can thus decrypt the message. This scenario ensures only the intended recipient can read the message, and
also give the recipient assurance as to the sender's identity. The speed and other advantages of using synchronous key encryption are
realized with this scenario.

Scenario 3: Biometric submission via proxy for non-computer based
Transactions

A parent asks his neighbor to pick up his child from a daycare center. The parent sends a message posting to the CBA with the following information:
-message identifier
-parent's (initiator) biometric sample
-name of neighbor (proxy)
-message to the daycare center: "please release my son"

The neighbor goes to the daycare center with the message identifier in hand. The daycare center operator submits the message identifier to the CBA, and the neighbor submits a biometric sample, which is also sent to the CBA. A match is performed, and if successful, returns the message "please release my son", along with the sender's name to the daycare center operator.

This scenario can be seen as a way to have a proxy represent someone for any reason (e.g., singing a legal contact, picking up a passport, etc.)

Scenario 4: Pure Verification of identity

Anytime identity is claimed and must be verified (cashing a check, applying for employment, EBT, etc) in every day life, a simple query to the CBA can be made. A submission and claimed identity are submitted to the CBA and a match score is returned.

Depending on the additional information stored by the CBA (and the level of identification that takes place during enrollment) additional information can be verified as well. This can include credit information (credit rating info), age (for access to bars) or other personal information. Permission to release such information would be inherent in the request (e.g., submitting the biometric is only done after understanding and approving release of the information being requested.

Unlocking the Private Key

Usually when biometric are discussed along side the topic of public key
infrastructure, the concept often relates to a sender using a biometric to unlock their private key from their smart card, hard drive, or where ever it may be stored. By protecting the private key with a biometric instead of a pin or password, the sender knows that if someone will not simply guess a password and initiate a message using their private key.

-- notes below--

The scenarios described above allow recipients to ensure that such
protection takes place (scenario 1) and allows the sender to know that only the recipient will read the message. In the case of today's PKI, these assurances are only as good as the PIN or password protecting the private keys. The CBA infrastructure actually identifies the senders and receivers, in addition to ensure that the messages have not been altered during transit.

If the sender can be assured that the receiver's private key is also secured by a biometric, then there is also an assurance that only the rightful recipient will read a message. It is very difficult to ensure levels of security at each recipient's site. There are issues with levels of identification as well. As opposed to a password, which provides a yes/no. It is impossible, however, to ensure that every recipient will protect their private key with a biometric, and to ensure that the system is set to. This biometric on the senders side to unlock a private key

Level of Identification

When issuing a certificate to a new enrolling a new user, diff/varying levels of identification scrutiny will be used depending on

Trusted Third party

Was it issued in a bona fide manner. Is it being used for a particular action, is it still good?

For any given transaction, send:

-Measurement of the biometric submission, or the submission itself

-Send the required threshold for verification or a request for score

There is little benefit for companies in building and maintaining databases of biometric enrollments. There is an inherent overhead and liability issues in keeping an up to date